

public notice describing the matching program. The notice should include:

1. The legal authority under which the match is being conducted.

2. A description of the matching program including whether the program is one time or continuing, the organizations involved, the purpose or purposes for which the program is being conducted, and the procedures to be used in matching and following up on the “hits.”

3. A complete description of the personal records to be matched, including the source or sources, system of records identifying data, date or dates and page number of the most recent FEDERAL REGISTER full text publication when appropriate.

4. The projected start and ending dates of the program.

5. The security safeguards to be used to protect against unauthorized access or disclosure of the personal records.

6. Plans for disposition of the source records and “hits.”

7. Agencies should send a copy of this notice to the Congress and to OMB at the same time it is sent to the FEDERAL REGISTER.

a. Agencies should report new or altered systems of records as described in subparagraph 5b, above, as necessary.

b. Agencies should also be prepared to report on matching programs pursuant to the reporting requirements of either the Privacy Act or the Paperwork Reduction Act. Reports will be solicited by the Office of Information and Regulatory Affairs and will focus on both the protection of individual privacy and Government’s effective use of information technology. Reporting instructions will be disseminated to the agencies as part of either the reports required by paragraph (p) of the Privacy Act, or section 3514 of Pub. L. 96–511.

8. *Use of Contractors.* Matching programs should, as far as practicable, be conducted “in-house” by Federal agencies using agency personnel, rather than by contract. When contractors are used:

a. The matching agency should, consistent with paragraph (m) of the Privacy Act, cause the requirements of that Privacy Act to be applied to the contractor’s performance of the matching program. The contract should include the Privacy Act clause required by Federal Personnel Regulation Amendment 155 (41 CFR 1–1.337–5).

b. The terms of the contract should include appropriate privacy and security provisions consistent with policies, regulations, standards, and guidelines issued by OMB, GSA, and the Department of Commerce.

c. The terms of the contract should preclude the contractor from using, disclosing, copying, or retaining records associated with the matching program for the contractor’s own use.

d. Contractor personnel involved in the matching program shall be made explicitly aware of their obligations under the Privacy Act and of these guidelines, agency rules, and any special safeguards in relation to each specific match performed.

e. Any disclosures of records by the agency to the contractor should be made pursuant to a “routine use” (5 U.S.C. 552a(b)(3)).

F. *Implementation and Oversight.* OMB will oversee the implementation of these guidelines and will interpret and advise upon agency proposals and actions within their scope, consistent with section 6 of the Privacy Act.

APPENDIX F TO PART 323—LITIGATION STATUS SHEET

1. Case Number.¹

2. Requester.

3. Document Title or Description.²

4. Litigation.

a. Date Complaint Filed.

b. Court.

c. Case File Number.¹

5. Defendants (DoD Component and individual).

6. Remarks (brief explanation of what the case is about).

7. Court Action.

a. Court’s Finding.

b. Disciplinary Action (as appropriate).

8. Appeal (as appropriate).

a. Date Complaint Filed.

b. Court.

c. Case File Number.¹

d. Court’s Finding.

e. Disciplinary Action (as appropriate).

APPENDIX G TO PART 323—PRIVACY ACT ENFORCEMENT ACTIONS

A. *Administrative Remedies.* Any individual who feels he or she has a legitimate complaint or grievance against the Defense Logistics Agency or any DLA employee concerning any right granted by this DLAR will be permitted to seek relief through appropriate administrative channels.

B. *Civil Actions.* An individual may file a civil suit against DLA or its employees if the individual feels certain provisions of the Privacy Act have been violated (see 5 U.S.C. 552a(g), reference (b).)

C. *Civil Remedies.* In addition to specific remedial actions, the Privacy Act provides for the payment of damages, court cost, and attorney fees in some cases.

D. *Criminal Penalties—*

¹Number used by the Component for reference purposes.

²Indicate the nature of the case, such as “Denial of access,” “Refusal to amend,” “Incorrect records,” or other violations of the Act (specify).

1. The Privacy Act also provides for criminal penalties (see 5 U.S.C. 552a(1).) Any official or employee may be found guilty of a misdemeanor and fined not more than \$5,000 if he or she willfully discloses personal information to anyone not entitled to receive the information, or maintains a system of records without publishing the required public notice in the FEDERAL REGISTER.

2. A person who requests or obtains access to any record concerning another individual under false pretenses may be found guilty of a misdemeanor and fined up to \$5,000.

APPENDIX H TO PART 323—DLA EXEMPTION RULES

Exempted Records Systems. All systems of records maintained by the Defense Logistics Agency will be exempt from the requirements of 5 U.S.C. 552a(d) pursuant to 5 U.S.C. 552a(k)(1) to the extent that the system contains any information properly classified under Executive Order 12958 and which is required by the Executive Order to be kept secret in the interest of national defense or foreign policy. This exemption, which may be applicable to parts of all systems of records, is necessary because certain record systems not otherwise specifically designated for exemptions herein may contain isolated items of information which have been properly classified.

a. ID: S500.10 (Specific exemption).

1. *System name:* Personnel Security Files.

2. *Exemption:* Investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, Federal contracts, or access to classified information may be exempt pursuant to 5 U.S.C. 552a(k)(5), but only to the extent that such material would reveal the identity of a confidential source. Therefore, portions of this system may be exempt pursuant to 5 U.S.C. 552a(k)(5) from the following subsections of 5 U.S.C. 552a(c)(3), (d), and (e)(1).

3. *Authority:* 5 U.S.C. 552a(k)(5).

4. *Reasons:* (i) From subsection (c)(3) and (d) when access to accounting disclosures and access to or amendment of records would cause the identity of a confidential source to be revealed. Disclosure of the source's identity not only will result in the Department breaching the promise of confidentiality made to the source but it will impair the Department's future ability to compile investigatory material for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, Federal contracts, or access to classified information. Unless sources can be assured that a promise of confidentiality will be honored, they will be less likely to provide information considered essential to the Department in making the required determinations.

(ii) From (e)(1) because in the collection of information for investigatory purposes, it is not always possible to determine the relevance and necessity of particular information in the early stages of the investigation. In some cases, it is only after the information is evaluated in light of other information that its relevance and necessity becomes clear. Such information permits more informed decision-making by the Department when making required suitability, eligibility, and qualification determinations.

b. ID: S500.20 DLA-I (Specific exemption).

1. *System name:* Criminal Incident/Investigations File.

2. *Exemption:* This system of records is exempted from the following provisions of the Title 5, United States Code, section 552a: (c)(3); (d); and (e)(1).

3. *Authority:* 5 U.S.C. 552a(k)(2).

4. *Reasons:* Granting individuals access to information collected and maintained by this component relating to the enforcement of criminal laws could interfere with orderly investigations, with the orderly administration of justice, and possibly enable suspects to avoid detection or apprehension. Disclosure of this information could result in the concealment, destruction or fabrication of evidence and jeopardize the safety and well being of informants, witnesses and their families, and law enforcement personnel and their families. Disclosure of this information could also reveal and render ineffectual investigative techniques, sources and methods used by this component and could result in the invasion of privacy of individuals only incidentally related to an investigation. Investigatory material is exempt to the extent that the disclosure of such material would reveal the identity of a source who furnished the information to the Government under an express promise that the identity of the source would be held in confidence, or prior to September 27, 1975 under an implied promise that the identity of the source would be held in confidence. This exemption will protect the identities of certain sources who would be otherwise unwilling to provide information to the Government. The exemption of the individual's right of access to his records and the reasons therefore necessitate the exemptions of this system of records from the requirements of the other cited provisions.

c. ID: S100.50 DLA-GC (Specific exemption).

1. *System name:* Fraud and Irregularities.

2. *Exemption:* This system of records is exempt from the provisions of 5 U.S.C. 552a(c)(3), (d)(1) through (4), (e)(1), (e)(4)(G), (H), and (I), and (f).

3. *Authorities:* 5 U.S.C. 552a(k)(2) and (k)(5).

4. *Reasons:* From subsection (c)(3) because granting access to the accounting for each